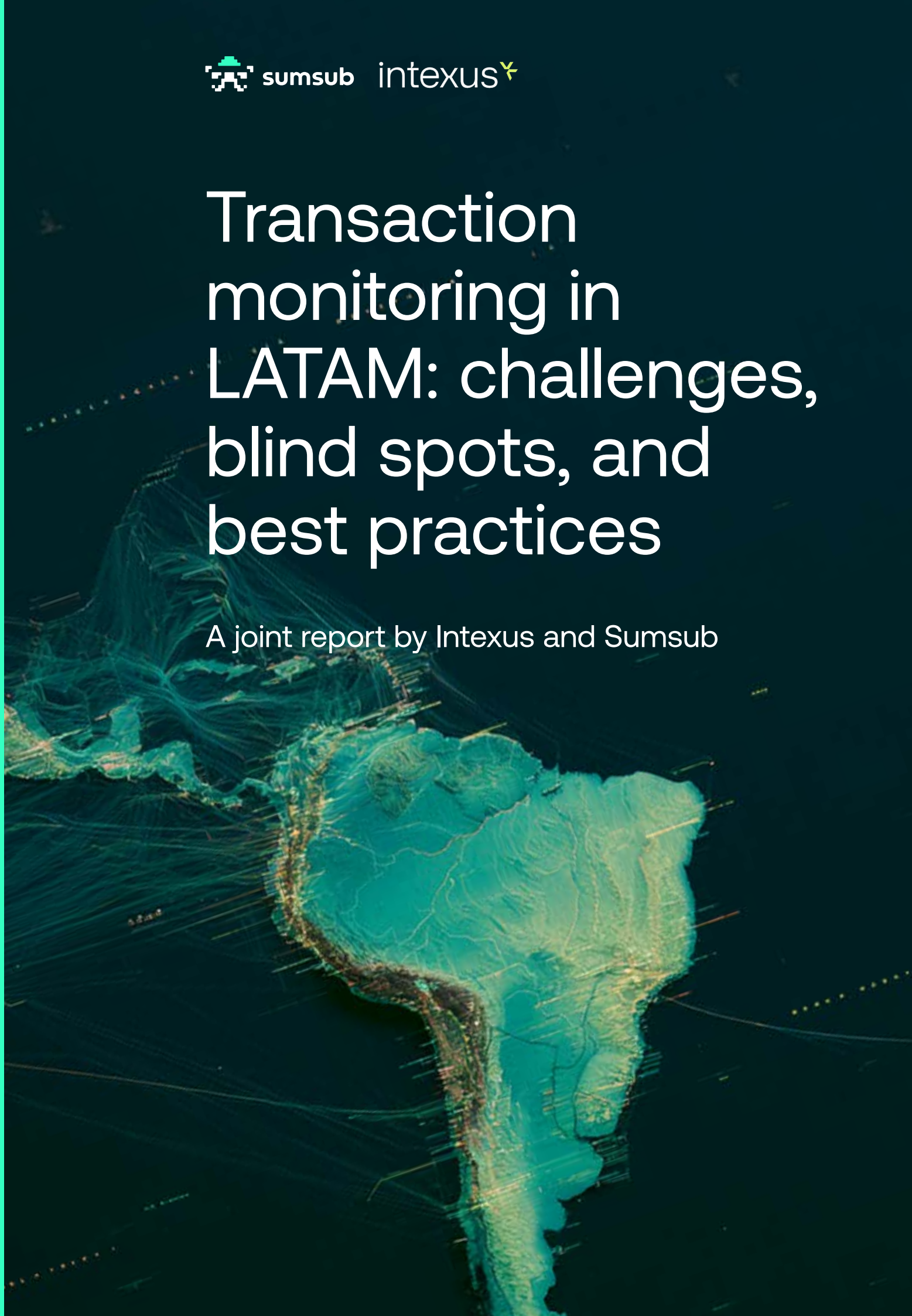
sumsub intexus

Transaction monitoring in LATAM: challenges, blind spots, and best practices

A joint report by Intexus and Sumsub

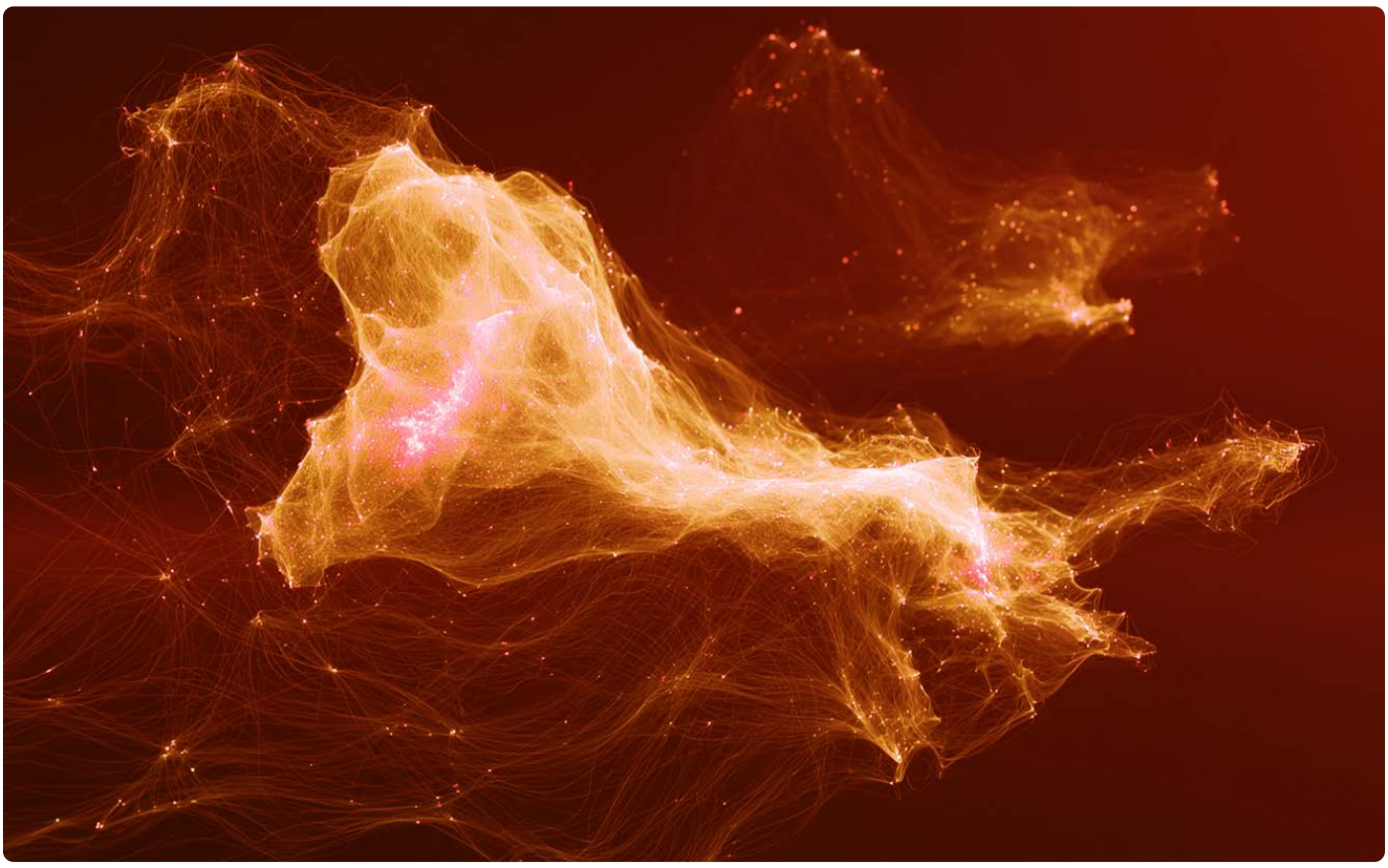


About this report

90 to 95% of alerts from legacy monitoring rules in Latin America are false positives. Nine in ten, sometimes nineteen in twenty.

Financial crime compliance costs the region's institutions somewhere around 15 billion dollars a year. Budgets keep rising for nearly every institution, leadership keeps pushing to cut them, and the region still sits below the world average on AML effectiveness.

For banks adapting to real-time rails. For fintechs and wallets handling high transaction volumes, crypto platforms moving between digital assets and local fiat, and compliance leaders who want benchmarks they can use.



Five takeaways:

1. Real-time payments are scaling up AML exposure faster than screening frameworks can absorb, and 2025 proved it with attacks on shared payment infrastructur
2. Legacy rules create massive false positive volumes, which burns out analysts and builds backlogs
3. Fraud and AML teams are increasingly overlapping, since scam proceeds and laundering flows run through the same accounts
4. Institutions lack unified customer risk visibility, a gap criminals deliberately exploit
5. Continuous monitoring is replacing static, one-time reviews as regulators tighten expectations

Why transaction monitoring is harder in LATAM

Cash everywhere, fintech adoption exploding, instant payments, crypto, all inside a few years. Monitoring tools built for slower, more uniform markets struggle here, partly because the data they expect (stable salaries, formal employment, consistent banking history) often does not exist for large parts of the population.

Mule account networks, digital smurfing, localized corruption, cross-border layering, trade-based schemes, fast crypto-to-fiat movement. Illegal mining, drug trafficking, organized crime, migration flows, and constant transaction exposure for anyone operating across borders. GAFILAT, the regional FATF body, keeps flagging the same weaknesses in its evaluations: thin beneficial ownership registries, underpowered FIUs, and supervision that lags the market.

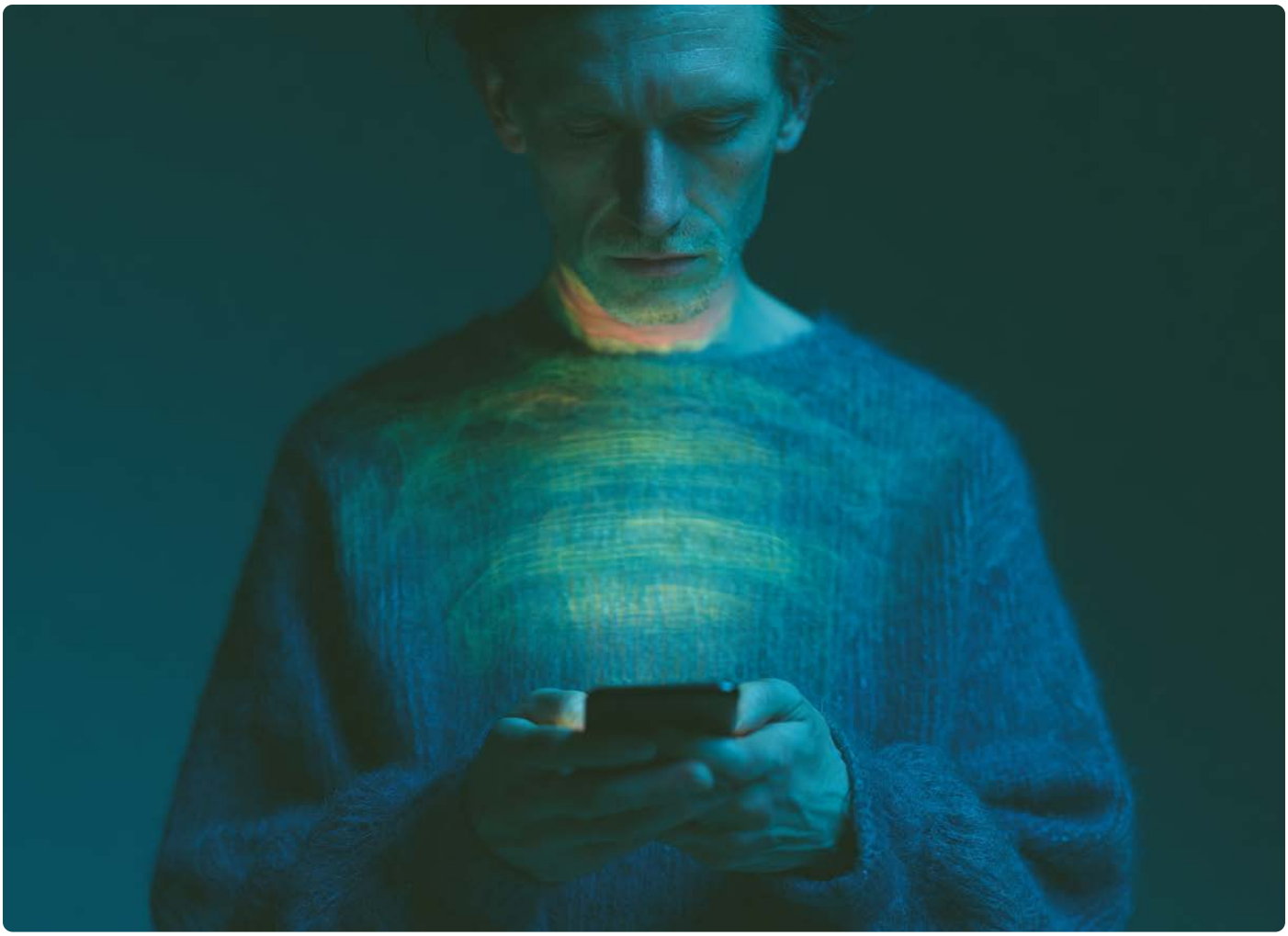
Venezuela, Haiti, and Nicaragua carry some of the worst corruption scores anywhere. Haiti ranks near the bottom of AML risk indexes globally and has not prosecuted a single money laundering offense successfully in five years. Corruption and laundering risk move together, no surprise there.

Bolivia went on the FATF grey list in June 2025, due to weak supervision and beneficial ownership gaps. Same month, US FinCEN designated three Mexican financial institutions as primary money laundering concerns over cartel-linked flows, cutting them off from US correspondent banking (so, access to dollars, gone). FATF also adopted revised payment transparency standards in June 2025, which will raise the bar for cross-border data quality over the coming years.

How the region fragments, country by country

Each market pulls compliance teams in a slightly different direction, and 2025 was a busy year for all of them, namely:

Country	Key AML focus	Monitoring challenge
Brazil	Pix ecosystem monitoring and mule account mitigation	Tens of billions of Pix transactions a year, single-day peaks above 250 million. Pix Automático (June 2025) adds a recurring pull-payment surface to watch.
Mexico	Cash-to-digital tracking and CNBV fraud prevention alignment	Heavy scam volume (59% of consumers targeted monthly) concealing cash laundering. The mid-2025 CNBV federal AML law overhaul expanded obligations.
Colombia	Open API payment rails and cross-border layering	Data fragmented across open banking pilots, and Bre-B, the instant payment system live since 2025, will replay Brazil's velocity problem.
Argentina	Crypto-to-fiat flows and informal currency matching	Volatility pushes users to unmonitored digital assets, so clean source-of-wealth records are hard to build. The CNV's 2025 regime brings virtual asset providers into supervision.
Chile	Criminalization of fraudulent payment credentials	Strict obligations to flag bad actors fast, with open finance rules (issued 2025) adding data-sharing duties.



Peru sits outside the table, but not the problem, mandating two-factor authentication after a sharp rise in cybercrime. An institution operating across three of these markets carries three rulebooks at once.

Most fraud here starts on mobile, a footprint unlike any other region. BioCatch's 2025 LATAM fraud research: 88% of fwraudulent sessions on mobile devices, malware climbing fast. Device intelligence, malware detection, behavioral session data (monitoring without them runs half blind).

The biggest monitoring blind spots today

Legacy rules and alert fatigue

90 to 95% false positives. Rigid static thresholds, duplicated alert logic, manual review overload, analyst burnout, backlogs that keep growing. Fewer than one or two alerts in a hundred ever turn into a suspicious activity report at many institutions, and almost nobody runs above-the-line and below-the-line testing to check whether thresholds sit anywhere near the right place. Segmentation, another quiet failure: a street vendor and a mid-size importer judged against the same amount threshold, which guarantees a mess of noise and missed cases at the same time.

Many institutions quietly optimize for regulatory defensibility over detection quality. Wide, inefficient rules to satisfy old audit checklists, and all that noise becomes a smokescreen real criminals break through.

Fragmented customer visibility

Onboarding KYC sits disconnected from transaction monitoring, fraud teams work apart from AML teams. Analysts cannot spot when a low-risk profile starts behaving like a laundering operation, and the fraud-AML split means scam proceeds get refunded or written off without anyone tracing where the money went next.

Monitoring without identity context, reactive by design. Deep checks on day one, then nothing (the one-and-done trap), and the expected activity declared at onboarding rarely gets compared against what the account does in month six.

When compliance can’t keep up with the rails

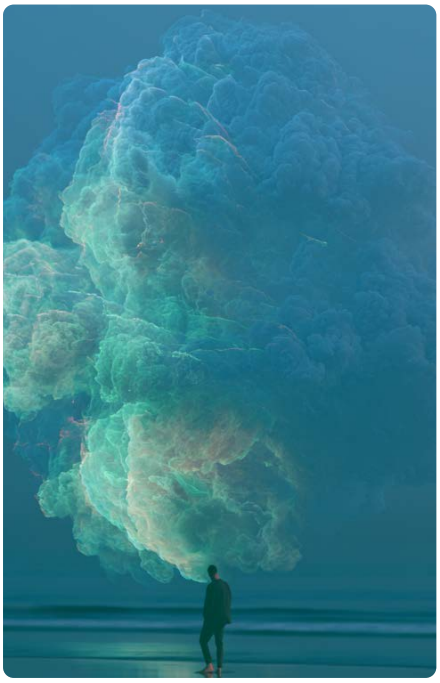
Pix, SPEI, instant transfers, wallet ecosystems. Money moves in seconds while risk reviews run in batches, hours or days behind, and Pix alone clears tens of billions of transactions a year. That’s Brazil, a cautionary tale and proving ground at the same time.

July 2025

Attackers diverted well over 100 million dollars from bank reserve accounts through C&M Software, a technology provider connecting institutions to Pix (reported figures vary, all of them ugly).

September 2025

Sinqia, a second provider, hit for about 130 million dollars using valid credentials, some two dozen banks exposed through a single point of failure. Both times the money was mule-networked and converted to crypto faster than any batch process could react. Brazil’s central bank then capped transaction values for institutions connecting through technology providers and now requires those providers to seek authorization.



The silo effect, an architectural race condition we keep seeing in LATAM expansions. Payment provider integrated for Pix rails, isolated KYC vendor on the side. Transactions credited instantly, before compliance can flag a CPF mismatch, the AML violation done before remediation can begin.

65%

Around 65% of institutions name poor data quality and fragmented integration as a major barrier to effective monitoring. Build versus buy belongs here too: in-house rule engines rarely scale alongside rising transaction volumes, and they tend to fail mid-growth, once the team that built them has moved on.

Typologies institutions keep missing

Built to look normal to a threshold-based system. The tells only show up when identity, device, and transaction data bundle up together.

Mule networks and account cycling

Valid individual accounts used collectively to split and cycle funds the moment they land. Dormancy followed by sudden bursts, fan-in fan-out patterns where many senders feed one account that empties within minutes, and balances that hover near zero.

Gen-AI fraud

Generated profiles that clear basic onboarding checks and cost institutions billions globally. Sumsub's 2025 fraud research points to deepfake-driven attacks as one of the fastest-growing vectors in the region, which puts pressure on liveness checks, not just document checks.

First-party fraud

Legitimate account holders claiming a transaction was unauthorized after falling for a scam. Hard to catch with rules alone, since the account history is genuinely clean right up to the dispute.

Digital smurfing and funnel accounts

High volumes of small deposits spread across regions, funneled into one account to dodge local reporting thresholds. Geographic dispersion of cash deposits against a single beneficiary is the signature.

Crypto layering

Passing fiat into localized crypto wallets to break the audit trail, often through P2P exchanges and stablecoins, which makes wallet attribution and blockchain analytics part of the monitoring job whether an institution touches crypto directly or not.

What effective monitoring programs look like

Unified, identity-centric compliance

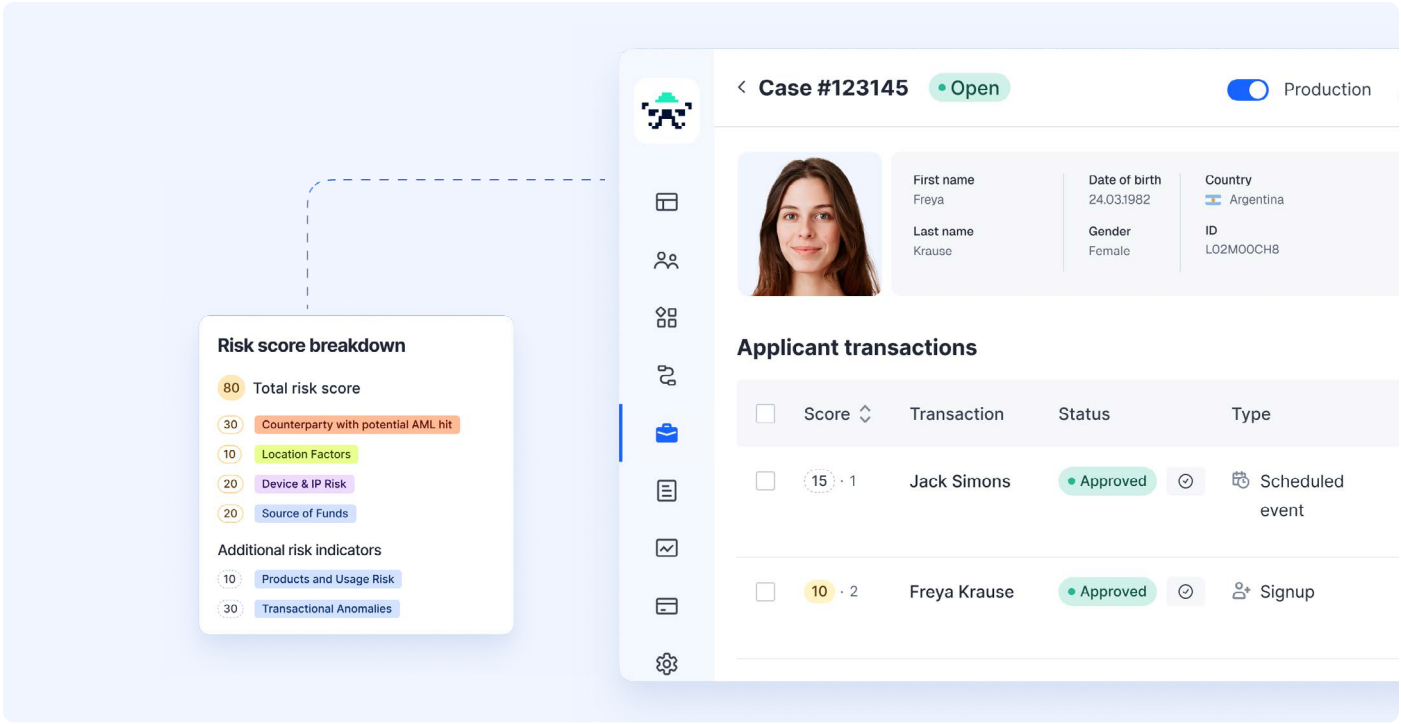
Transaction patterns change, the risk profile updates automatically across every system. The declared profile from onboarding (occupation, expected volumes, source of funds) are next to live behavior, so deviations surface on their own. Orchestration platforms covering the full customer lifecycle make this far easier than stitching point tools together (we have watched the stitching approach fail more often than it works). In the end, what's expected is an onboarding identity data and transaction monitoring as one operational stream.

Smarter alert management

Contextual alerting groups related alerts into a single case file instead of peppering analysts with hundreds of repetitive notifications. The AI part, to be clear: filter out the 95% of noise, reduce analyst overload, let human teams investigate the complex, high-risk cases.

This process begins with measurement first. Alert-to-case and case-to-report conversion, time to disposition, backlog age, rules tuned against those numbers on a fixed cadence (the annual audit is too late).

Then feedback: investigator outcomes flow back into the rules and models, so a pattern closed as a false positive a hundred times stops generating alert number one hundred and one. Regulators across the region increasingly ask how models are governed and whether decisions can be explained. Explainability designed in from day one, since bolting it on later costs more and convinces nobody. Together, these are dynamic, behavior-based thresholds, behavioral analytics, and AI-assisted prioritization.



Real-time risk operations

Real-time screening is the regulatory baseline now, with sanctioned parties kept out of the system entirely, even temporarily, which batch processing cannot promise. Continuous behavioral monitoring and live payment velocity analysis can catch automated mule transfers as they happen, and escalation or fund holds fire automatically the moment high-risk velocity patterns reveal themselves.

Brazil's Pix special refund mechanism (MED) gives this a regulatory anchor; victims request recovery, the receiving institution blocks funds immediately, and none of it works unless detection fires within minutes. Same logic at the exit door. Offboarding, finding and removing high-risk accounts (mule accounts above all), has become as critical as onboarding, and payment screening belongs in the same flow, counterparties, payment references, receiving institutions, checked in real time, before settlement.

A monitoring maturity model

Most LATAM institutions we see remain somewhere between reactive and structured:

Stage	Core operational characteristics	Technology stack focus
Reactive	Manual processes relying completely on static, legacy rules	Spreadsheet trackers, hardcoded single-amount thresholds, siloed tools
Structured	Centralized transaction monitoring across core systems	Batch-processing rule engines, shared databases, basic case management
Proactive	Dynamic customer risk scoring based on updated profiles	Connected KYC-transaction tools, automated risk adjustments
Adaptive	AI-assisted continuous monitoring with real-time risk responses	Real-time orchestration platforms, AI anomaly detection, contextual alerts

LATAM case studies

These case studies are anonymized, per their request.

A digital bank cuts alert fatigue

- → A fast-growing fintech, transaction volumes surging, legacy rules drowning analysts in false positives.
- → Backlogs past regulatory reporting windows (the point where alert fatigue turns into a compliance breach waiting to happen).
- → Static thresholds with dynamic behavioral rules and AI-prioritized alert workflows.
- → False positive volume down 10% in the first year, automated onboarding pass rates from 40% to 90% through smart routing without widening risk tolerance, manual report compilation time down 90% via automated formatting for local regulatory filings.

Dismantling a cross-border mule network

An institutional wallet network, targeted by an organized ring running synthetic profiles and distributed mule accounts, funds split and moved across borders under standard limit alerts.

→ Each account unremarkable on its own, which is exactly the design.

→ Live transaction velocity, device fingerprints, and onboarding identity histories cross-referenced on one timeline.

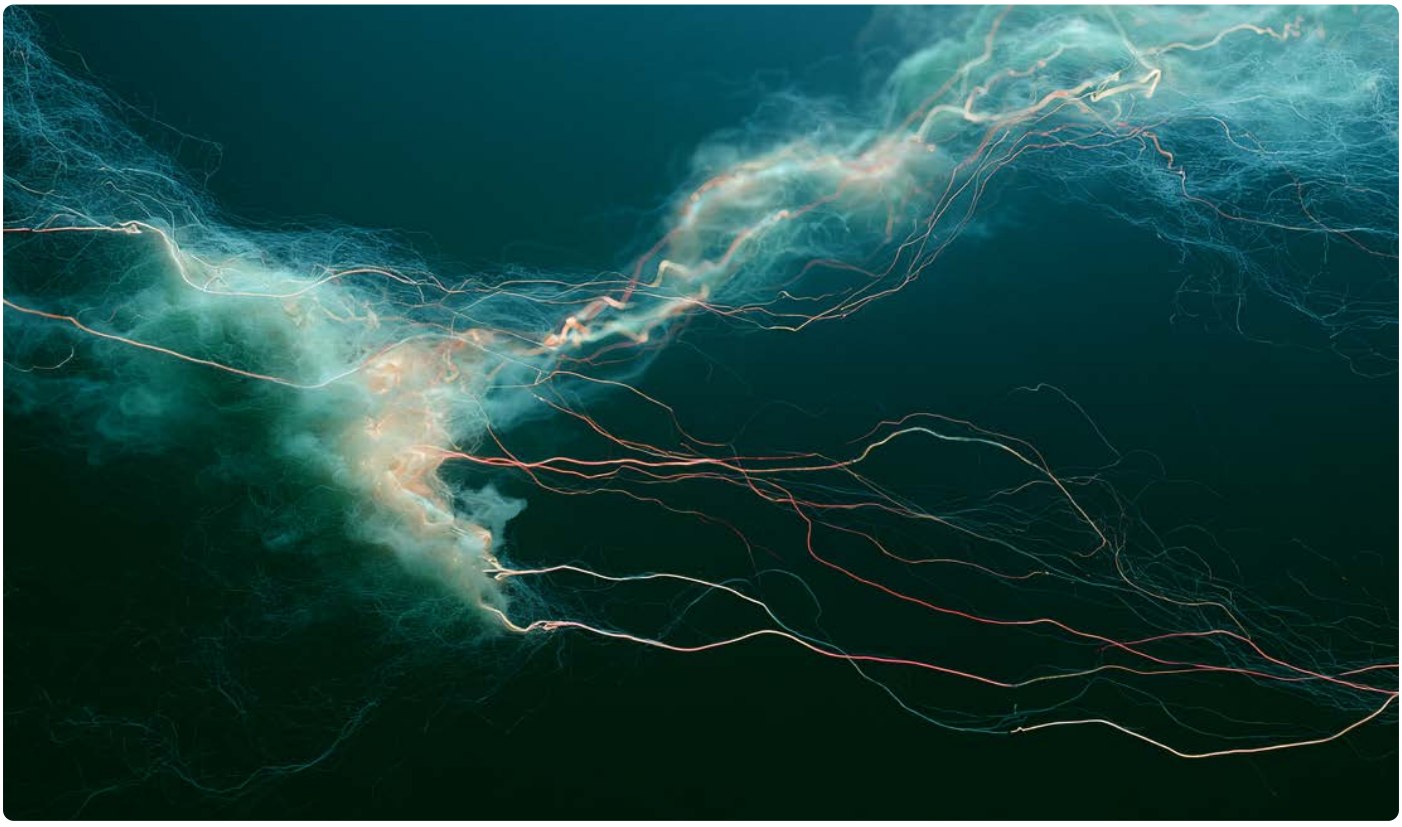
→ Dozens of seemingly unrelated accounts linked through shared devices and overlapping payment counterparties, digital smurfing caught in real time, the network frozen within minutes instead of days.

→ The FIU report got substance out of it too, named linkages and device evidence, no vague pattern descriptions.

Looking ahead

Automated alert summarization, investigation copilots, predictive typology recommendations, all landing in the next 12 to 24 months. **Cloud-native monitoring already holds around 63.8% of the global market**, midsize banks running millions of real-time screenings at a fraction of on-premise costs, and the r**eal-time payments market is projected to grow at nearly 47% a year.**

Fraud detection has become the fastest-growing application on transaction monitoring platforms, overtaking AML as the main reason institutions invest. Identity, fraud, and AML, one operational layer. Brazil's Meu BC, launched in December 2025, lets citizens block their CPF from being used to open new accounts, and institutions must check that database first.

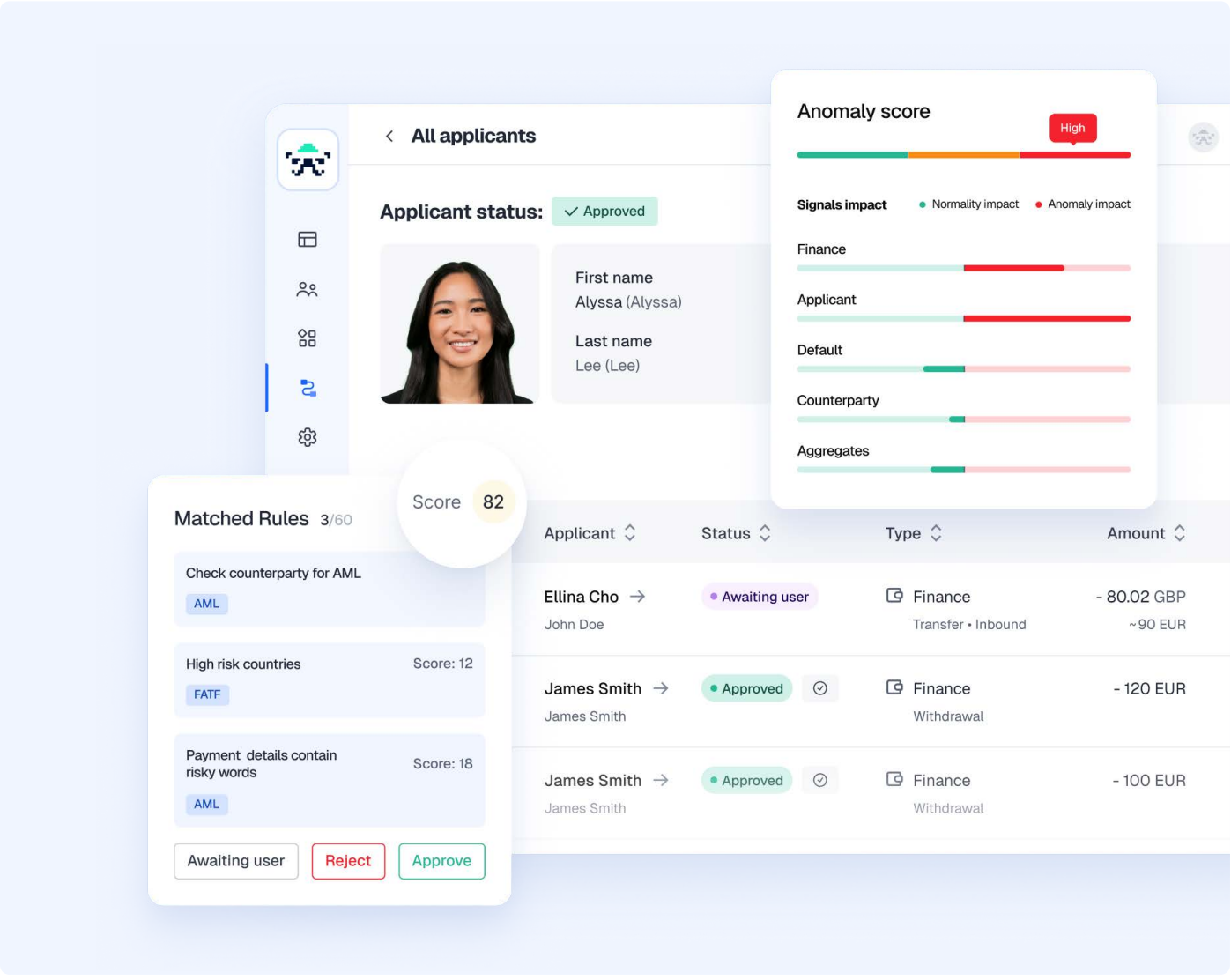


Brazil's central bank published its rules for crypto service providers in November 2025, in force early 2026, stablecoin and exchange flows pulled into the supervised perimeter. FATF's revised payment transparency standards (June 2025) will force better originator and beneficiary data on cross-border payments. Grey-listing pressure after Bolivia's June 2025 addition gives every supervisor in the region a reason to tighten.

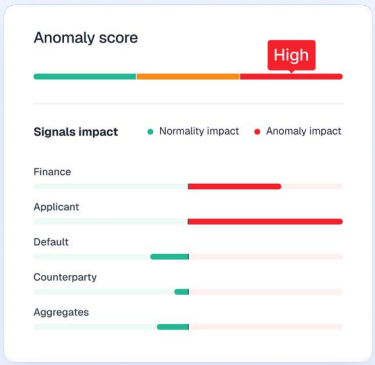
Institutions that keep relying on fragmented, reactive monitoring models will struggle to keep pace with real-time financial ecosystems. Fines, reputational damage, lost correspondent relationships, criminal networks that learn faster than rule libraries.

Where Sumsub fits in

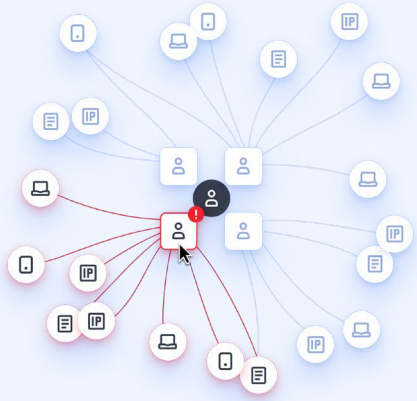
Sumsub is a single verification platform built around this kind of integrated workflow. About 10 years in the market, more than 4,000 companies served, over 2 billion identities processed, and around 690,000 fraud attempts prevented every month. User verification, business verification, AML transaction monitoring, fraud prevention, and travel rule compliance, all on one shared data layer, so onboarding data feeds monitoring rules natively, with no custom integration project in between.



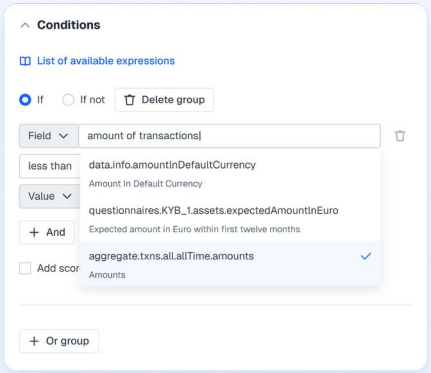
For a LATAM institution, the most relevant pieces are:



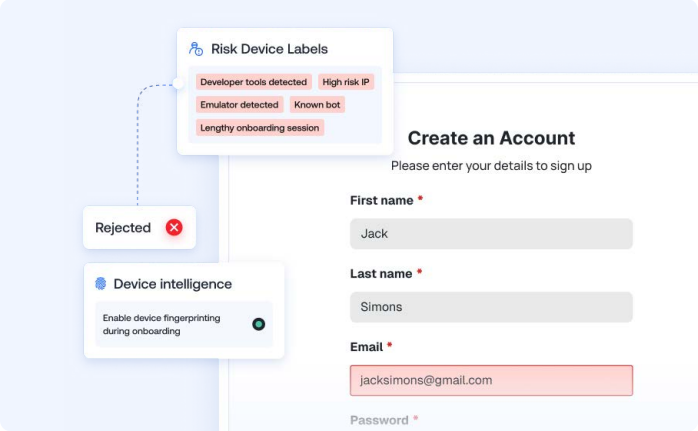
AML transaction monitoring: real-time monitoring with 300+ pre-built rule bundles, dynamic risk scoring, and FIU report generation in formats like goAML, STR, and SAR



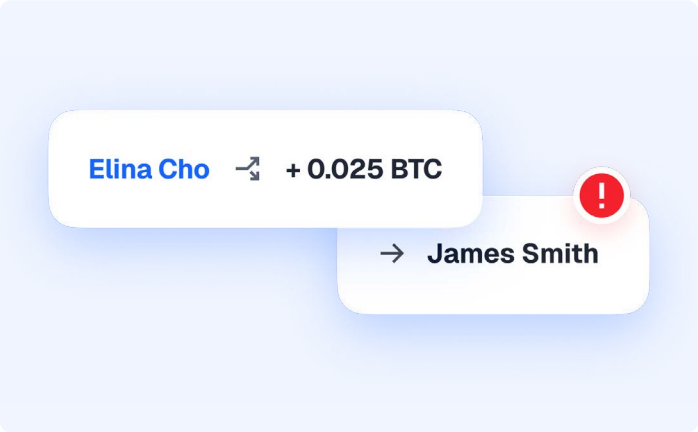
Fraud prevention: identity fraud, multi-accounting, account takeovers, payment fraud, and money mule detection, enriched with device fingerprinting and behavioral signals



A **rules engine** without coding, including rules built from plain-English prompts, so compliance teams can test and adjust thresholds in minutes



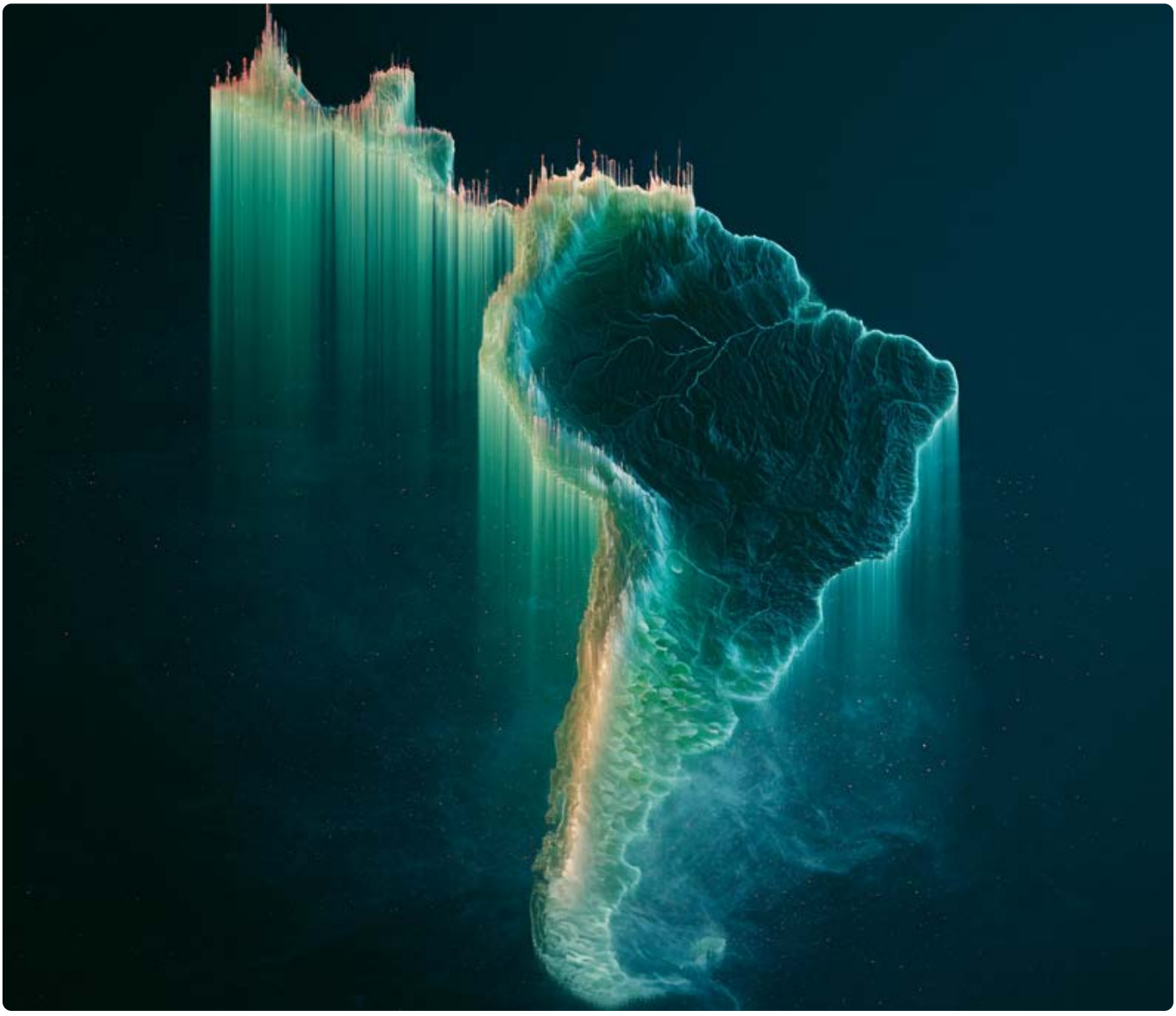
Transaction network analysis that links accounts through device fingerprints, IP addresses, and counterparty IDs on interactive graphs, with cases generated automatically from alerts



Coverage across fiat and crypto, including crypto-to-fiat transactions, blockchain analysis, and wallet attribution

Where Intexus fits in

Intexus brings the local layer that global platforms cannot supply on their own: regional market intelligence and operational context drawn from working inside LATAM compliance environments every day. A platform sets the speed of your monitoring, and people who work in these markets every week are the ones who know what to watch for, and in what form supervisors expect to see it.

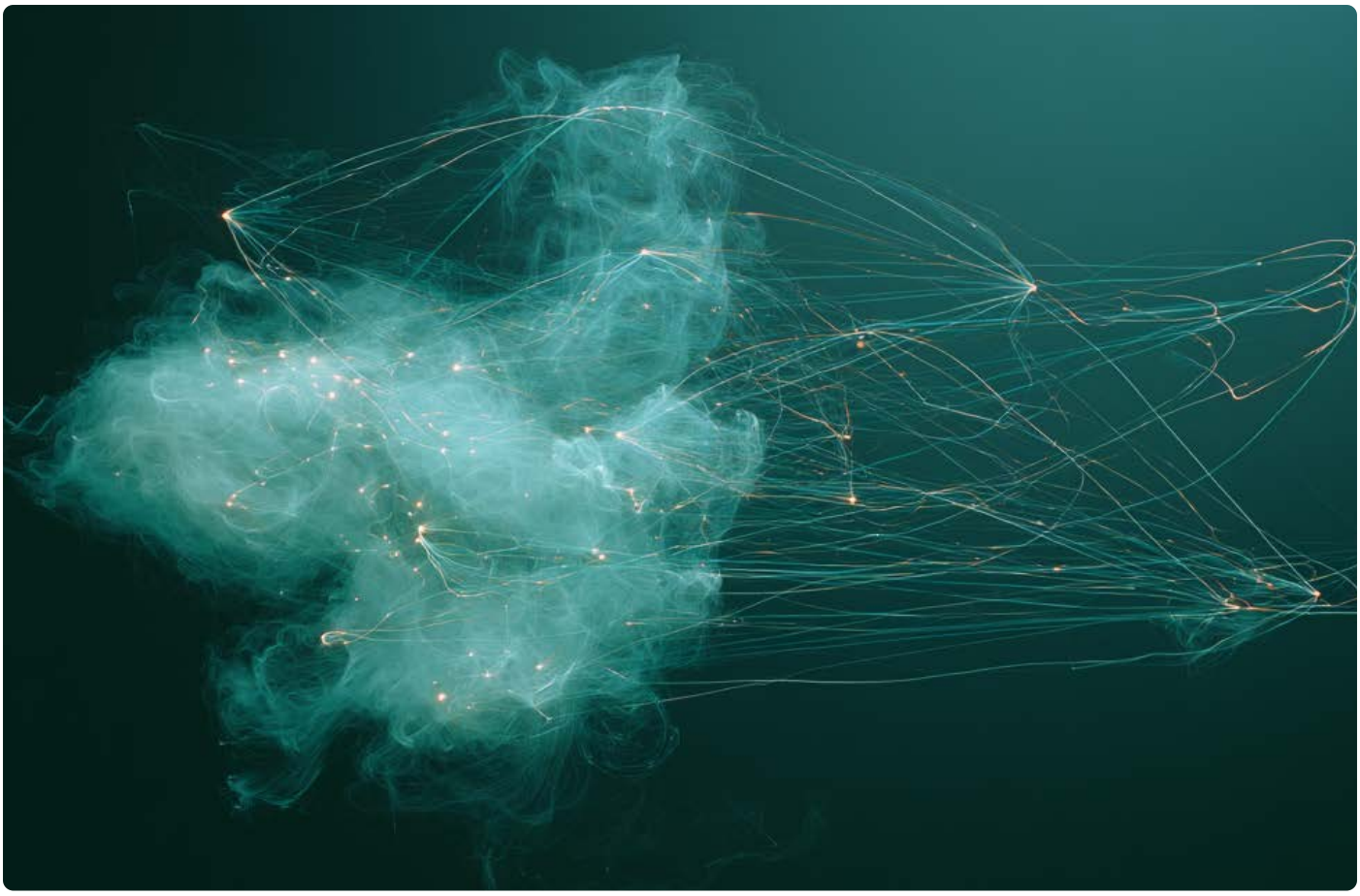


Intexus understands the practical requirements regional regulators and supervisors expect, including:

- → **AML/CFT regulatory context and enforcement trends** across LATAM, from FATF and GAFILAT findings down to country supervisor priorities
- → **Country-level compliance observations and operational realities**, like how FIU reporting works in practice, market by market, deadlines and formats included
- → **Regulatory evolution and policy direction**, including the 2025 wave of instant payment, crypto, and AML law changes covered in this report
- → **Regional financial crime typologies and the patterns behind them**, grounded in local cases, since imported global templates tend to miss them
- → **Monitoring program design** that fits local rails like Pix, SPEI, and Bre-B

This local knowledge improves the quality and credibility of compliance programs, license applications, and regulator relationships. Paired with a unified verification platform, it gives institutions both the technology and the regional judgment to run identity-centric monitoring that holds up.

Keep your business compliant and safe from financial crime with Intexus and Sumsub



About Intexus

Intexus is a Latin American consultancy focused on AML/CFT, compliance operations, and financial crime prevention across the region, providing localized market intelligence and regulatory expertise.

About Sumsub

Sumsub is a global verification platform that covers user verification, business verification, AML transaction monitoring, fraud prevention, and travel rule compliance. Sumsub is recognized as a Leader in the Forrester Wave for Identity Verification Solutions, Q3 2025, and in Gartner's Magic Quadrant for Identity Verification, 2025, for the second consecutive year.

Try Sumsub

Book a demo →